**CYBER SECURITY TIPS**
SDPD Neighborhood Policing Resource Team
April 9, 2012

**CONTENTS**

Reporting Attempted Sexual Exploitation
Preventing Cyber Crimes
Additional Information
Protecting Your Children's Identities

Because we as individuals and businesses rely on computers for nearly everything in our daily lives, we need to be aware of the risks of using computers and to take appropriate measures to minimize the dangers. Among these dangers are viruses that erase or corrupt information in computers, viruses that infect computers and then propagate and infect other computers, hackers that break into computers and create mischief or steal information, employees who steal confidential business information, predators who attempt to meet and sexually exploit children, etc. This paper contains cyber security tips for protecting against viruses and spyware, preventing and dealing with ID theft, using the Internet, preventing Wi-Fi hacking, and dealing with hotspot dangers. It also contains a variety of specific tips for businesses and parents. Many of these tips also apply to text messaging.

Persons interested in general information on cyber security and tips on general security topics, dealing with attacks and threats, e-mail and communications, mobile devices, privacy, safe browsing, software, and applications should go to the website of the Computer Emergency Readiness Team of the U. S. Department of Homeland Security at **www.us-cert.gov/cas/tips**.

## PROTECTING AGAINST VIRUSES AND SPYWARE

The following measures can help protect your computer from viruses and spyware:

- Keep your computer up to date with the latest firewalls and anti-virus, anti-spyware, and anti-adware software. The latter are designed to protect against software that either self-installs without your knowledge or is installed by you to enable information to be gathered covertly about your Internet use, passwords, etc. This kind of software is often installed when you visit websites from links in e-mails. Use security software that updates automatically. Visit **www.OnGuardOnline.gov** for more information. This also applies to multi-function printers, fax machines, and copiers that can be accessed using a web browser.
- Do not open any e-mail from an unknown sender. Delete it without opening it. "Drive-by spam" can automatically download malware when an HTML e-mail is opened. You don't have to click on a link or open an attachment to get infected. Another way to prevent this kind of attack is to deactivate the display of HTML e-mails and display e-mails in pure-text format only.
- Businesses should also install real-time e-mail and web security along with solutions that prevent data theft and loss of confidential information. Traditional anti-virus and spyware products don't provide this protection.
- Use security software that updates automatically. Visit **www.OnGuardOnline.gov** for more information.
- Do not buy or download free anti-spyware software in response to unexpected pop-ups or e-mails, especially ones that claim to have scanned your computer and detected malicious software.
- Make sure the pop-up blocker in the tools menu of your browser is turned on. This will prevent most pop-up ads. If you do get one, be careful in getting rid of it. Never click on any of its boxes. By clicking on No or Close you may actually be downloading malware onto your computer. And even clicking on the X in the upper right-hand corner can initiate a download instead of closing the ad. To be safe on a PC, hold down the Ctrl and Alt keys and hit Delete. Then in the Windows Security box click on Task Manger, and then click on End Task. This will clear your screen. Then run a full anti-virus scan.
- Do not respond in any way to a telephone or e-mail warning that your computer has a virus even if it appears to come from an anti-virus software provider like Microsoft, Norton, or McAfee. "Helpful hackers" use this ploy to get you to download their software to fix the virus or sell you computer monitoring or security services to give them remote access to your computer so they can steal your passwords, online accounts, and other personal information. If you already have anti-virus software on your computer you'll receive a security update or warning directly on your computer.
- Use the latest versions of Internet browsers, e.g., Microsoft Internet Explorer 8, which is designed to prevent phishing attacks. Use Explorer in the "protected mode," which restricts the installation of files without the user's consent, and set the "Internet zone security" to high. That disables some of Explorer's less-secure features. And set your operating system and browser software to automatically download and install security patches.

- Do not install files or programs from CDs or flash drives before checking them for viruses.
- Scan demo disks from vendors, shareware, or freeware sources for viruses.
- Avoid using electronic bulletin boards.
- Do not download files from unknown sources.
- Do not allow any website to install software on your computers.
- Scan downloaded files for viruses. Avoid downloading executable files.
- Businesses should obtain copies of your anti-virus software for your employees' home computers if your employees do some business work at home. Also ensure that your employees' home computers are protected by hardware and software firewalls between their system(s) and the Internet.

## PREVENTING AND DEALING WITH IDENTITY THEFT

Every person who willfully obtains personal identifying information, e.g., name, address, date of birth, Social Security Number (SSN), mother's maiden name, etc. as defined in Cal. Penal Code Sec. 530.5(b), and uses that information for any unlawful purpose is guilty of a public offense. Identity theft is the fastest growing crime in the United States. Every year about 15 million people become victims. Everyone is vulnerable. Skilled identity thieves use a variety of methods to steal your personal information. These include the following:

- Dumpster diving. They rummage through trash looking for bills and other paper with your personal information on it.
- Skimming. They steal credit- or debit-card numbers with a special storage device when processing your card.
- Phishing, spear phishing, smishing, vishing, and whaling. They send realistic-looking e-mail that asks recipients to go to a bogus website and provide personal information, use text messages instead of e-mails, and send fake e-mails to high-ranking executives to trick them into clicking on a link that takes them to a website that downloads software that secretly records keystrokes and sends data to a remote computer over the Internet.
- Changing your address. They divert your billing statements to another location by completing a change-of-address form.
- Stealing. They steal wallets, purses, mail (credit card and bank statements, pre-approved credit offers, new checks, tax information, etc.), employee personnel records, etc.

An enormous amount of information is available on various identity theft issues. Much of this is summarized in this section, which contains tips for minimizing risk, things to do if you become a victim or are notified of a security breach involving personal information, and links to many websites. For comprehensive set of links to the websites of a wide range of government agencies and nonprofit organizations that deal with these issues, go to The Consumer Federation of American's website at **idtheftinfo.org**. It contains links that deal with consumer, business, and victim resources, shopping for identity theft services, protecting yourself, statistics and studies, etc.

### Protecting Personal Information

- Give out credit or debit card, bank account, and other personal information only when you have initiated the contact or know and trust the person you are dealing with. Beware of e-mail or telephone promotions designed to obtain personal information.
- Put strong passwords on your credit card, bank, computer, and online accounts. Avoid using easily remembered numbers or available information like mother's maiden name, date of birth, phone number, or the last four digits of your SSN. Passwords should be more than eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol. Use of non-dictionary words is also recommended. Other advice on creating strong passwords can be found at **www.microsoft.com/protect/yourself/password/checker.mspx**.
- Select password reset questions whose answers cannot be found online or from other research tools. Don't compromise a strong password with an easily answered reset question like: What is your mother's maiden name?
- Use different passwords for banking, e-commerce, e-mail, and other accounts.
- Memorize your passwords. Don't carry them in your purse or wallet.
- Keep personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your home.

- Make sure that the copying machines used by you and others who have your personal data, e.g., tax preparers, have data security measures installed to prevent unauthorized access to data on the copier's disk.
- Protect you health insurance cards like you would your credit or debit cards. If asked for your policy numbers or any other personal information in a doctor's office, make sure no one else is near enough to hear or see them.
- Protect your Medicare card number as you would your SSN. Don't give it to anyone who offers free medical equipment or services and then requests your number. And don't let anyone borrow or pay to use your Medicare card. That's foolish and illegal.
- Shred or tear up any documents with personal or financial information before throwing them in the trash. Use a cross-cut shredder.
- Avoid all online games and quizzes that request personal information, including your e-mail address. Providing this information can put your identity at risk.

**Using Credit and Debit Cards**

- Never loan your card to anyone.
- Pay attention to billing cycles. Check with the credit card company if you miss a bill to make sure that your address has not been changed without your knowledge.
- Only put the last four digits of your account number on checks you write to your credit card company. It knows the whole number and anyone who handles your check as it is processed won't have access to the number.
- Notify your credit card companies and financial institutions in advance of any address or phone number changes.
- Bring home all card receipts and match them against your monthly statements. Look for charges you didn't make.
- Dispose of card receipts at home. Never toss them in a public trash container.
- Call the credit card company or bank involved if a new credit card you applied for hasn't arrived in a timely manner.
- Monitor the expiration dates of your cards and contact the card issuer if new cards are not received before your card expires.
- Report all lost or stolen cards immediately and request cards with new numbers. In this case the federal Truth in Lending Act limits your liability to $50 of any charges made before you report your card lost or stolen. Contact the issuer if replacement cards are not received in a reasonable time.
- Sign and activate new cards promptly on receipt. Or write "See ID" on the signature line on the back of the card. Then a thief won't have your signature. A merchant will ask you for a picture ID to make sure you are the cardholder.
- Never put a card number on a post card or on the outside of a mailing envelope.
- Make sure only the last four digits of your card number show up on your receipts. Use of full card numbers on electronically printed receipts is prohibited by California law. (Note that the merchant copy can show the full credit card number.) Report non-complying businesses to the Methamphetamine Strike Force hotline at **(877) 662-6384**.
- Cancel accounts you don't use or need. Carry only the cards and identification you need when you go out.
- Tear into small pieces or shred any pre-approved credit card offers. They can be used by thieves to order cards in your name.
- Ask your credit card company to stop sending blank checks.
- Have your name removed from lists supplied by the Consumer Credit Reporting Companies (Equifax, Experian, and TransUnion) to be used for pre-approved/pre-screened offers of credit or insurance. Call **(888) 567-8688** or go to **www.optoutprescreen.com** to do this.
- Don't let your card out of sight. A person taking it to a Point of Sale (POS) device might have a skimmer to steal the information on the magnetic strip, copy your card number and the 3-digit security number on the back of the card, or switch cards. If you do give your card to a waiter or other sales person, make sure you get your card back. And use a credit card instead of a debit card whenever possible. With the former you don't have to pay disputed charges. But with the latter it may take the bank about two weeks to restore the funds to your account.
- Make sure your bank and credit card companies have your latest home and cell phone numbers, and e-mail address so they can contact you quickly if they suspect fraud in your accounts.

- Some credit cards now have embedded Radio Frequency Identification (RFID) chips that are designed to be read by secure card readers at distances of less than 4 inches when properly oriented for "contactless payments." Thus, RFID readers that are available to the general public and can operate at ranges up to 25 feet and are essentially useless in stealing the information on your card. And even if that information is "hi-jacked," the cards are said to have security features that make it difficult or impossible to make a fraudulent transaction. Furthermore, the information is on the chip is not the same as that on the magnetic strip, and it cannot be used to create a functioning counterfeit version of the card. If you have a card with a RFID chip and don't want to risk having the information on it stolen and used in any fraudulent activity, ask your card company for a new card without a chip.
- Beware of skimmers on self-checkout terminals at grocery stores, gasoline pumps, and other places where you might swipe your credit or debit card. Things to watch for are listed below under Using an ATM.

**Protecting Your U.S. Passport:**

- Since August 2007 all passports issued by the U.S. State Department have a small contactless RFID computer chip embedded in the back cover. They are called "Electronic or e-passports." The chip stores the same data that is visually displayed on the photo page of the passport. It also stores a digital photograph of the holder, a unique chip identification number, and a digital signature to protect the stored data from alteration. Unauthorized reading of e-passports is prevented by the addition of a radio-frequency blocking material to their covers. The passports cannot be read until they are physically opened. Then there are protocols for setting up a secure communication channel and a pair of secret cryptographic keys in the chip to ensure that only authorized RFID readers can read the data on the chip.
- In July 2008 the U.S. State Department began issuing U.S. passport cards that can be used to enter the United States from Canada, Mexico, the Caribbean, and Bermuda at land border crossings or seaports of entry that are less expensive that a passport book. It cannot be used for international travel by air. To increase speed, efficiency, and security at U.S. land and sea border crossings the card contains a RFID chip. However, no personal information is on the chip. It only points to a record stored at secure U.S. government databases. And a protective RFID-blocking sleeve is provided with each card to prevent unauthorized reading or tracking of the cared when it is not in use. Make sure you carry the card in the sleeve.

**Protecting Your Social Security Number**

- Examine your Social Security Personal Earnings and Benefits Estimate Statement for possible fraud. You will receive it about three months before your birthday each year.
- Provide your SSN only when it is required by a government agency, employer, or financial institution. In a recent case a man received a call from a person who claimed to be a jury coordinator and said that a warrant has been issued for his arrest because he failed to report for jury duty. When he protested that he never received a summons he was asked for his SSN and date of birth to verify the records. Caught off guard he provided this information. Instead he should have hung up realizing that court workers would never ask for a SSN or other personal information.
- In a variation of the above scam, the caller says that you've been selected for jury duty and asks you to verify your name and SSN. Remember, notification of jury duty is always done by mail.
- Never use your SSN for identification. Don't carry it or your Social Security card in your purse or wallet.
- Do not have your SSN or driver's license number printed on your checks. And never write your SSN on a check.
- Provide your driver's license or some other identification number when reporting a crime in which you are the victim. Do not provide your SSN. The crime report will be available to the defense if a suspect is prosecuted.

**Managing Your Accounts**

- Keep a record in a secure place of all your credit and debit card, and bank and investment account phone numbers for quick reference if identity theft occurs.
- Review your bank statements carefully. Match your checkbook entries against paid checks. Look for checks you didn't write.
- Never leave transaction receipts at bank machines or counters, trashcans, gasoline pumps, etc.

**Carrying Personal Information in a Purse or Wallet**

- Carry only a driver's license, cash, and one credit card. Don't carry blank checks or a checkbook. Don't carry anything with a PIN written on it.
- Keep a record of its contents. Photocopy both sides of your credit and debit cards and driver's license and keep them in a safe place at home.
- Don't carry your Social Security card or anything with your SSN on it. Persons with Medicare cards should carry photocopies of the cards with the last four digits of their SSN removed. Keep the card is a safe place at home.
- If you carry a wallet in a purse, keep credit or debit cards in separate compartment and not in your wallet.
- Don't carry personal information of your family members.
- Don't carry any account or computer passwords.
- Take the measures listed below for victims of identity theft if your wallet is lost or stolen. Don't wait for someone to find and return it. These include filing a police report, reporting your credit and debit cards missing, closing checking accounts, having a fraud alert placed on your credit reports, notifying your medical insurance companies, reporting a missing driver's license, etc.

**Using the Mail**

- Deposit outgoing mail at a Post Office, in a blue U.S. Postal Service collection box, or give it directly to your mail delivery person. Put it in a collection box only if there is another pickup that day. It is not safe to leave mail in a box overnight. Also, do not leave mail for pickups from personal curbside boxes or cluster box units.
- Pick up your mail as soon as possible after it arrives in your personal curbside box or cluster box unit. If this is not possible, have a trusted friend or neighbor collect your mail, especially if you are expecting a box of checks or a new credit or debit card.
- Consider having new checks mailed to your bank for collection to avoid possible theft from your mailbox.
- Use a locked mailbox and make sure the lock works.
- Investigate immediately if bills do not arrive when expected, you receive unexpected credit cards or account statements, you are denied credit for no apparent reason, and you receive call or letters about purchases you did not make.
- Report the non-receipt of expected valuable mail by calling the sender and the Postal Inspection Service as soon as possible.

**Using an ATM**

- Use ATMs that are inside a store or a bank. These are less likely to have been tampered with for skimming, which is the illegal capture and utilization of a cardholder's financial information from an ATM transaction. If you use an outside ATM, it should be well-lighted and under video surveillance.
- Get off your cell phone and be alert when using an ATM.
- Check the machine and everything around it before you take out your card. Look for parts that seem crooked or have a different color, or decals that are partially covered. If something doesn't seem right, go to another machine.
- Most ATMs have flashing lights in the card slot. Their obscuration is a sign of tampering.
- Look to see if there is anything in the slot where you insert your ATM card. Thieves place a small, hard-to-detect skimming device in the card slot to steal your PIN and other bank account information. If anything looks suspicious, give it a pull or push. Skimmers are usually held in place loosely by glue or tape to make them easy for the thief to remove. If you remove one, contact the SDPD immediately. Don't throw it away or keep it; that would make it look like you are running the scheme.
- Check for a false keypad that has been installed over the built-in one. False keypads stick out too far or look strange.
- Check the area around the machine for hidden cameras. To be safe shield your hand when entering your PIN so it can't be seen by anyone near you or by a hidden camera.
- If you use a debit card memorize your PIN and keep it secret. Don't write it down or keep it in your wallet or purse.

- Keep the customer-service phone numbers of your bank and credit-card company readily available. Call the appropriate number immediately if your card gets stuck in an ATM. Do not leave the ATM.
- Don't leave your transaction receipts at the ATM. Take them home and use them in balancing your account.
- Monitor your bank statements frequently and report any unauthorized activity immediately.

**Buying Identity Theft Protection**

- You cannot buy absolute protection against identity theft. Beware of any such claims, especially regarding prevention of misuse of existing credit-card accounts, theft of medical records, and theft of personal information from employer's personnel files.
- Before signing up for protection, be sure to understand what services are provided, what protections they afford, and how the personal information you provide is protected.
- Fraud alerts, which provide some protection against fraud in opening new accounts that require credit reports, do not provide absolute protection and only deal with a small fraction of identity theft incidents.

**Checking for Possible Identity Theft**

- Obtain free copies of your credit reports from the three nationwide consumer credit reporting bureaus (Equifax, Experian, and TransUnion) by visiting **www.AnnualCreditReport.com** or calling **(877) 322-8228**. This is the ONLY source of free reports authorized under Federal law. You can get one free report annually from each bureau. Stagger your requests to obtain one every four months. That way you can monitor your credit during the year. Check these reports for errors, fraudulent activities, e.g., accounts opened without your knowledge or consent, and persons or businesses checking on your credit. Contact the reporting bureau immediately if you see any inaccuracies. These bureaus may also try to sell you credit monitoring products or services for a fee. The FTC requires that any advertising for such products or services be delayed until after you get your free credit reports.
- Be aware that if you order a free credit report from an unauthorized website such as **freecreditreport.com** you will be given a free limited-time trial membership in its credit monitoring service that will provide daily monitoring of your credit reports, alert notices of key changes, bi-monthly credit scores, etc. If you don't cancel this membership you will be charged a fee for each month that you remain a member. Before becoming a member you need to understand exactly what protection and services it will and will not provide, and whether you need the additional protection. Some services you will pay for you can do yourself at no cost, e.g., ordering credit reports and placing fraud alerts.
- These websites are required to print a disclosure that states the following at the top of each page that mentions free credit reports: "THIS NOTICE IS REQUIRED BY LAW. Read more at **www.FTC.gov**. You have the right to a free credit report from **www.AnnualCreditReport.com** or **(877) 322-8228**, the ONLY authorized source under federal law." They are also required to include a clickable button to "Take me to the authorized source" and clickable links to **www.AnnualCreditReport.com** and **www.FTC.gov**. However, neither of these requirements is enforced by the FTC so they don't appear on websites that advertise free credit reports.
- Place a security freeze on your credit reports. This will protect you against fraud in new accounts by prohibiting the credit reporting bureaus from releasing your credit reports to a potential creditor without your express permission. Go to their websites for the procedures and fees for placing and lifting freezes. Their addresses are: **www.equifax.com**, **www.experian.com**, and **www.transunion.com**.
- Check your medical bills and health insurance statements to make sure the dates and types of services match your records. Read every letter you get from your insurer, including those that say "this is not a bill." If you see a doctor's name or date of service that isn't familiar, call the doctor and your insurer.
- Once a year request a list of all benefits paid in your name by your health insurer. If the thief has changed your billing address you would not be receiving any bills or statements.

**If You Become a Victim**

File a police report as soon as possible if you become or may become a victim of identity theft. Call the SDPD non-emergency number, **(619) 531-2000** or **(858) 484-3154**. Then do the following:

- Set up a folder where you can keep a log of all your reports and supporting documents, and contacts and their phone numbers.
- Contact the FTC to report the theft. Its Identity Theft Hotline is **(877) 438-4338**. Or visit its website at **www.ftc.gov/idtheft**. The FTC is the federal clearinghouse of complaints of victims of identity theft. It helps victims by providing information to resolve financial and other problems that could result from identity theft. Its booklet entitled *Take Charge: Fighting Back Against Identity Theft* deals with bank accounts and fraudulent withdrawals, bankruptcy fraud, investment fraud, phone fraud, and other specific problems. It also describes the immediate steps victims should take and ways to minimize recurrences.
- Report the theft to the fraud units of Equifax at **(800) 525-6285**, Experian at **(888) 397-3742**, and TransUnion at **(800) 680-7289**. Ask to have a fraud alert placed on your credit reports. It will tell creditors to follow certain procedures before they open new accounts in your name or make changes to you existing accounts. In placing a fraud alert you will be entitled to free copies of your credit reports. Review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Fraud alerts are good for 90 days and can be renewed. They are free.
- Alert your banks of any fraud and request new account numbers with new checks, ATM cards, and PINs. Also provide new passwords and stop payment on any missing checks.
- Contact all your creditors by phone and in writing to inform them of the fraud.
- Call your credit card companies and request account number changes. Don't ask to cancel or close your accounts; that can hurt your credit score, especially if you have outstanding balances. Say you want a new numbers issued so your old numbers will not show up as being "cancelled by consumer" on your credit reports. Also change your PINs and passwords.
- Call the security or fraud departments of each company you have a charge account with to close any accounts that have been tampered with or established fraudulently. Follow up the request in writing and ask for written verification that the accounts have been closed and any fraudulent debts discharged. Keep copies of all documents and records of all conversations about the theft. If you still want a charge account, request a new number.
- Report the loss of your SSN to the IRS. This will alert the IRS that someone might use your SSN to get a job or file a tax return to receive a refund. Call its Identity Theft Hotline at **(800) 908-4490** and go to **http://www.irs.gov/privacy/article/0,,id=186436,00.html.** Follow the directions there regarding identity theft and your tax records, and the need to provide it with proof of your identity. And read "Ten Things the IRS Wants You to Know about Identity Theft" on its main website at **www.irs.gov**. Also contact the Social Security Administration (SSA) on its Fraud Hotline at **(800) 269-0271** or by e-mail to the Office of the Inspector General at **www.ssa.gov/org**.
- Call the U.S. Secret Service at **(619) 557-5640** if the crime involves counterfeit credit cards or computer hacking.
- Contact the California DMV Fraud Hotline at **(866) 658-5758** to report the theft and see if another driver's license has been issued in your name.
- Notify the U.S. Postal Inspector if your mail has been stolen or tampered with. Its number is **(626) 405-1200**. Or report it online at **http://postalinspector.uspis.gov**.
- In the case of medical identity theft request a copy of your current medical files from each health care provider, and request that all false information be removed from your medical and insurance files. Enclose a copy of the police report with your requests. For more information things to do if you are a victim of medical identity theft or concerned about it go the World Privacy Forum's website at **www.worldprivacyforum.org/ medicalidentitytheft.html**.
- Call the Health Insurance Counseling and Advocacy Program's Senior Medicare Patrol (HICAP/SMP) at **(800) 434-0222** to report any fraud involving Medicare.
- If you are contacted by a collector for a debt that resulted from identity theft, send the debt collector a letter by certified mail, return receipt requested, stating that you did not create the debt and are not responsible for it. Include a copy of the police report you filed for the identity theft crime and a completed copy of the FTC's Identity Theft Victim's Complaint and Affidavit. It can be downloaded from its website at **www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf**. Also write in your letter that you are giving notice to a claimant under California Civil Code Sec. 1798.93(c)(5) that a situation of identity theft exists.

- Other things you should do as a victim are in the Identity Theft Victim Checklist on the website of the California Office of Privacy Protection at **www.privacy.ca.gov/cis3english.htm**. It's website at **www.privacy.ca.gov** contains additional tips on avoiding and resolving identity theft problems.

Another useful website is that of the Identity Theft Resource Center (ITRC) at **www.idtheftcenter.org**. It contains information ranging from advice for people who have had a wallet stolen to tips for reducing the risks of identity theft. It also contains fact sheets, solutions to various identity theft problems, letter forms, scam alerts, a "Help, I'm a Victim of Identity Theft" button, and answers to frequently asked questions. Its toll-free victim-assistance number is **(888) 400-5530**.

**If You Are Notified of a Security Breach Involving Personal Information**

Most states now have security breach notification laws under which a person whose personal information is compromised must be notified of the breach. The California Breach Notification Law is in Civil Code Sections 1798.29, 1798.82, and 1798.84. The first applies to state government agencies; the other two apply to any person or business doing business in the state. The notice requirement is triggered if the breach involves a person's name in combination with any of the following: SSN; driver's license or California Identification Card number; financial account, credit card, or debit-card number along with any PIN or other access code required to access the account; medical information; or health insurance information. You should do the following for each and also be alert for possible spear phishing as defined above under Internet fraud and other crimes:

- SSN. Put a fraud alert on your credit reports at Equifax, Experian, and TransUnion, and order copies of your reports. Review them carefully and file a police report if you find anything suspicious. If you don't find anything suspicious at first, renew the fraud alert and check your credit reports periodically. Also report the loss to the IRS and SSA.
- Driver's License or California Identification Card number. Call the DMV Fraud Hotline to report the incident.
- Financial account numbers. Call the institution to request new account numbers and PINs. And put new passwords on your accounts.
- Medical or health insurance information. Review your explanation of benefits statements and contact your insurer if you see any services you did not receive.

For additional information on this and other privacy issues visit the Privacy Rights Clearinghouse's website at **www.privacyrights.org**.

**USING THE INTERNET**

In 2009 the Internet Crime Complaint Center (IC3), which acts in partnership with the National White Collar Crime Center and the FBI, received more than 336,000 complaints on its website and referred over 146,000 to law enforcement agencies for further consideration. The total loss from all of these cases was over $560 million. You may be at risk if you answer "yes" to any of the following questions:

- Do you visit websites by clicking on links within an e-mail?
- Do you reply to e-mails from persons or businesses you are not familiar with?
- Have you received packages to hold or ship to someone you met on the Internet?
- Have you been asked to cash checks and wire funds to someone you met on the Internet?
- Would you cash checks or money orders received through an Internet transaction without first confirming their legitimacy?
- Would you provide your personal banking information in response to an e-mail notification?

If you become a victim of Internet fraud or receive any suspicious e-mails you should file a complaint with the IC3 at **www.ic3.gov**. Its website also includes tips to assist you avoiding a variety of Internet frauds. You should also contact your e-mail provider. Most keep track of scams. Send your provider the suspicious message header and complete text. For more information on Internet fraud visit **www.LooksTooGoodToBeTrue.com**.

The following material deals with several specific kinds on Internet fraud and other crimes: e-mail scams and malware, online shopping frauds, phishing, spear phishing, smishing, vishing, whaling, social network dangers, illegitimate websites, e-card dangers, and unsafe drugs from online pharmacies. A summary of safe cyber practices is also provided.

**E-mail Scams and Malware**

Cybercriminals use e-mail in many clever ways to try to take your money and identity, and disrupt your computer operation, gather sensitive information, or gain unauthorized access to your computer. To protect your assets and computer you should never reply, click on any links, or open any attachments of e-mails that offer great bargains or something that's not legal. And if you don't recognize the sender, you should delete the e-mail without even opening it. Be especially suspicious about the following:

- Business opportunities to make money with little effort or cash outlay
- Offers to sell lists of e-mail addresses or software
- Chain letters involving money
- Work-at-home schemes
- Health and diet claims of scientific breakthroughs, miraculous cures, etc.
- Get-rich-quick schemes
- Free goods offered to fee-paying group members
- Investments promising high rates of return with no risk
- Kits to unscramble cable TV signals
- Guaranteed loans or credit on easy terms
- Credit repair schemes
- Vacation prize promotions
- Special offers that require a credit check and a small fee for verification expenses to be paid by a credit or debit card
- Notices of prize or lottery winnings that require you to pay a fee to cover expenses
- Requests for personal or financial information

Regarding the latter, cybercriminals often pose as government agencies or financial institutions that you normally deal with. Remember that government agencies never send important things by e-mail, and your financial institutions already have your personal information.

If you suspect something might be a scam, check it out on Hoaxslayer at **www.hoax-slayer.com**. This website is devoted to debunking e-mail hoaxes and exposing Internet scams. It is constantly increasing its compiled list of scams.

**Online Shopping Frauds**

Do not use a debit card when shopping online, especially on an unfamiliar website. If something goes wrong your account can be emptied quickly without your knowledge. This can result in overdrafts, fees, and an inability to pay your bills. Even if your bank offers a fraud guarantee it is not obligated to restore your funds for at least two weeks while it investigates. If have to use a debit card, use one that is reloadable. Then you only risk the amount you put on the card if something goes wrong.

If you use a credit card the federal Fair Credit Billing Act limits your liability to $50 for any unauthorized or fraudulent charges made before you report the billing error. To protect yourself you need to do the following:

- Write to your credit card company within 60 days after the date of the statement with the error and tell it your name and account number, that your bill contains an error and why it is wrong, and the date and amount of the error.
- Pay all other charges. You do not need to pay the disputed amounts.

Consumers should be aware that if a deal looks too good to be true, it probably is. In one scam the victim located a car on the Auto Trader website and contacted the seller directly by e-mail. He was told that the car would be shipped to him for inspection and approval if he wired the money to a bank account where it would be held in escrow. He wired the money but the car never arrived. To prevent this kind of scam consumers need to be diligent in verifying all the parties involved in the purchase by phone calls, face-to-face meetings, etc. In a similar case the consumer asked to see the car before wiring any money. The scammer ended all contacts at that point.

Another example involved a Craigslist ad for a vacation apartment rental in New York City. The renter was told he had to act fast and wire the money or he'd lose out on this good deal. All three elements of a typical scam were present in this case: (1) act fast or lose the deal, (2) wire the money, and (3) a price that was too good to be true. Scammers also use Craigslist and other websites to advertise rentals in your area. They will make a duplicate of a legitimate ad but with a much lower price and a different contact number. They will ask for cash upfront without showing the property or ask you to fill out an application with your SSN or other personal information. These are signs of the scam.

Online scams also promise great deals on airline tickets, timeshare properties, and vacation packages. The biggest red flag is when payment is requested by a wire transfer. It's difficult to track these transfers and almost impossible to get a refund. Check out the company offering the deal before making a purchase. If it and the deal appear to be legitimate, pay by credit card and not by wire. Then if the deal turns out to be fraudulent, you can dispute the charges as indicated above.

**Phishing**

In an e-mail scam known as "phishing" identity thieves fish for personal information by sending realistic-looking e-mail that asks recipients to go to a bogus website and provide personal information such as a credit card number, password, or Personal Identification Number (PIN). Legitimate banks and financial institutions don't send e-mails asking you to verify your account information. They already have it. The following are examples of scammers posing as the Internal Revenue Service (IRS), Federal Bureau of Investigation (FBI), Federal Deposit Insurance Corporation (FDIC), and the Centers for Disease Control and Prevention (CDC).

Each year during tax preparation time there is a surge in the number of frauds by criminals posing as IRS officials to obtain personal information for identity theft. The IRS never sends out unsolicited e-mails or asks for detailed personal and financial information. Any such e-mail is a fraud. So are telephone calls from someone stating they are from the IRS. Go to the IRS website at **www.irs.gov** for information on the latest scams and instructions on how to protect yourself from suspicious e-mails or phishing schemes. The IRS also recommends forwarding the suspicious e-mail to it at **phishing@irs.gov**.

The growing popularity of tax preparation software has led to a rise in e-mail scams targeted at do-it-yourself taxpayers. The fraudulent e-mails claim to come from a software provider and might offer a software update or download. They may ask for personal financial information or other sensitive data and contain links to websites that could download malware. Legitimate software providers routinely send customers e-mails advising them of the status of their tax returns but never ask for sensitive personal data. Any software updates should be done on your provider's website or desktop product. Also, forward any suspicious e-mails to your software provider's security center.

Fraudulent e-mails have also been sent out by criminals posing as FBI agents and officials. They give the appearance of legitimacy by using the FBI seal, letterhead, and pictures of the FBI Director. They may also claim to come from the FBI's domestic or overseas offices. Like the IRS, the FBI does not send out e-mails soliciting personal or financial information. For more information on this kind of fraud go to the FBI website at **www.fbi.gov** and click on New E-Scams and Warnings under Be Crime Smart.

Another agency that has become aware of fraudulent e-mails in its name is the FDIC. These ask recipients to "visit the official FDIC website" by clicking on a hyperlink that directs them to a fraudulent website that includes hyperlinks that open a "personal FDIC insurance file" to check on their deposit insurance coverage. Clicking on these links will download a file that contains malicious software to collect personal and confidential information.

In 2009 the CDC issued a health alert warning people not to respond to an e-mail referencing a CDC-sponsored state vaccination program for the H1N1 (Swine Flu) contagion that requires registration on "www.cdc.gov." People that click on this embedded link risk having a malicious code installed on their computer. Examples of this and other hoaxes and rumors can be seen at **http://www.cdc.gov/hoaxes_rumors.html**.

Use the following tips to counter phishing:

- Do not open any e-mail from an unknown sender, especially if it offers something sensational, e.g., a video of Osama Bin Laden's death. Delete it without opening it. "Drive-by spam" can automatically download malware when an HTML e-mail is opened. You don't have to click on a link or open an attachment to get infected. Another way to prevent this kind of attack is to deactivate the display of HTML e-mails and display e-mails in pure-text format only.
- Do not open any unexpected e-mail attachments.
- Do not give out any passwords or personal information or click on any links no matter what the e-mail says, e.g., that you will be locked out of your account if you don't provide the information, or that you owe money.
- Do not click on links in e-mail messages purporting to come from your bank or any other institution or business that you have an account with. Retype the address into your browser. If you do click on a link and are prompted to log in with your password, don't do it. Close your browser and log into your account to make a payment or do whatever the message said.
- Do not double click on any Internet pop-up with a link to an offer or provide any personal information in response to a pop-up offer. And never enter personal information on a pop-up page.
- Use the latest versions of Internet browsers, e.g., Microsoft Internet Explorer 8, which is designed to prevent phishing attacks. Use Explorer in the "protected mode," which restricts the installation of files without the user's consent, and set the "Internet zone security" to high. That disables some of Explorer's less-secure features. And set your operating system and browser software to automatically download and install security patches.
- Make sure the website page you are entering sensitive information on is secure. You can tell it is secure when the address on the top of your screen where the Uniform Resource Locator (URL) is displayed begins with **https://** rather than **http://.** You can also look for a closed padlock or an unbroken key on the bottom of your screen to indicate the page is secure. If the lock is open the site or the key is broken, the page is not secure. Note that on many websites only the order page will be secure.
- Read the website's privacy policy. It should explain what personal information it collects, how the information is used, whether it is provided to third parties, and what security measures are used to protect the information. Consider taking your business elsewhere if you don't see, understand, or agree with the policy.
- Keep your computer up to date with the latest firewalls and anti-virus, anti-spyware, and anti-adware software. The latter are designed to protect against software that either self-installs without your knowledge or is installed by you to enable information to be gathered covertly about your Internet use, passwords, etc. This kind of software is often installed when you visit websites from links in e-mails. Use security software that updates automatically. Visit **www.OnGuardOnline.gov** for more information.
- Do not buy or download free anti-spyware software in response to unexpected pop-ups or e-mails, especially ones that claim to have scanned your computer and detected viruses.
- Make sure the pop-up blocker in the tools menu of your browser is turned on. This will prevent most pop-up ads. If you do get one, be careful in getting rid of it. Never click on any of its boxes. By clicking on No or Close you may actually be downloading malware onto your computer. And even clicking on the X in the upper right-hand corner can initiate a download instead of closing the pop-up. To be safe on a PC, hold down the Ctl and Alt keys and hit Delete. Then in the Windows Security box click on Task Manger, and then click on End Task. This will clear your screen. Then run a full computer security scan.
- Do not respond in any way to a telephone or e-mail warning that your computer has a virus even if it appears to come from an anti-virus software provider like Microsoft, Norton, or McAfee. "Helpful hackers" use this ploy to get you to download their software to fix the virus or sell you computer monitoring or security services to give them remote access to your computer so they can steal your passwords, online accounts, and other personal information. If you already have anti-virus software on your computer you'll receive a security update or warning directly on your computer.
- Look for valid trust marks to increase your confidence in using a website. Reputation trust marks like BBBOnline offer a basic level of proof that there is an actual business behind the website and that it follows

proper business practices. Privacy trust marks like TRUSTe indicate that the business is aware of identity theft and personal data abuse and abides by the requirements of the trust mark provider in its privacy policy. A Secure Socket Layer (SSL) trust mark like VeriSign indicates that the site uses up-to-date encryption technology to scramble communications between the website and your computer. And security-scanning trust marks like McAfee SECURE indicate that the business uses a regularly scheduled security auditing service for its website to ensure that it is free of viruses, spyware, adware, etc. Because a phisher could create a false trust mark and verification website, you cannot know that the mark is valid unless you click on it. A link will take you to the verification website of the trust mark provider. The trust mark is valid if its verification website has **https://** in its URL.

- Be careful in visiting websites that don't have trust marks.

**Spear Phishing**

This is a more sophisticated version of phishing. It targets groups of people who have something in common, e.g., they work for the same company, deal with the same financial institution, or attend the same college. The fraudulent e-mails come from organizations the potential victims would normally get e-mails from. Success in spear phishing depends on three things: (1) the apparent source of the e-mail must be a known and trusted individual or organization, (2) there is information in the e-mail that makes it look legitimate, and (3) the request for personal or company-privileged information, or direction to click on an included link must have a logical basis, e.g., to update usernames and passwords. The information needed for these things is obtained hacking into the organization's computer network, data breaches, or combing through other websites, blogs, and social networking sites. Here are some things to do to avoid becoming a spear phishing victim.

- Remember that most companies, banks, agencies, etc. don't request personal information by e-mail. If in doubt, call the sender. But don't use the number in the e-mail. It's usually phony too.
- Use a browser with a phishing filter.
- Never follow a link from an e-mail to a secure website. Enter the URL manually.

**Smishing**

This is phishing with text messages instead of e-mails. "Smishing" is a term coined from Short Message Service (SMS) and phishing. In these scams you may receive a SMS stating that your account will be charged for some particular program or purchase unless you visit a given URL within two days to cancel the order. When you click on the cancel link you will download malware to your computer. Do not respond to these SMSs. Alternatively, the SMS may give you a phone number to call where you will be asked for personal information. Before calling verify that the number matches the number of the named institution, e.g., your bank. And never give out personal information unless you have initiated the call.

**Vishing**

In this scam criminals use Voice over Internet Protocol (VoIP) technology to make telephone calls from anywhere in the world pretending to be a legitimate business, often using a fraudulent called ID matching the identity of the misrepresented company. The term "vishing" comes from voice phishing. It directs recipients to call an illegitimate telephone number where they are tricked into giving up personal financial information. They might receive an urgent recorded message telling them that their credit card has been compromised and directing them to call the following telephone number immediately and punch in their 16-digit account number to verify their identity. Alternatively, you may receive an e-mail asking you to call a particular number to prevent your account from being blocked. Someone there will attempt to get you to give up personal information. The best defense against vishing is to treat any unsolicited telephone message with suspicion and only give your personal information out when you have initiated the call and are sure the other party is legitimate.

**Whaling**

In another scam known as "whaling" fake e-mails have been sent to high-ranking executives to trick them into clicking on a link that takes them to a website that downloads software that secretly records keystrokes and sends

data to a remote computer over the Internet. This lets the criminal capture passwords and other personal or corporate information, and gain control of the executive's computer. In one case fake subpoenas have been sent to executives commanding them to appear before a grand jury in a civil case. The link that offers a copy of the entire subpoena downloads the malicious software.

**Social Networking Dangers**

Malware creators, identity thieves, and spammers are increasingly targeting users of social networking sites in an effort to steal personal data and account passwords. One of the tactics they use to gain access to this information involves sending social networking users e-mails that appear to come from online friends. For example, some Facebook users have been receiving e-mails from their "friends" that claim to contain a video of them. When they click on it they download malware that installs a malicious program on their hard drive. A virus known as Koobface sends itself to all the friends on the victim's Facebook profile. A new version of the virus also is affecting users of MySpace and other social networking sites. Cyber-criminals are tricking social networking users into downloading malicious software by creating fake profiles of friends, celebrities, and others. Security experts say that such attacks, which became widespread in 2008, are increasingly successful because more and more people are becoming comfortable with putting all kinds of personal information about themselves on social networking sites. They warn that users need to be very careful about what information they post because it can be used to steal their identities. Facebook users should become a fan of its security page at **www.facebook.com/security**, which has posts related to all sorts of security issues, tips, resources, and other information.

To avoid problems on social networks or anywhere in the Internet, users should:

- Never post any information that you don't want made public. Once it's posted you cannot retract it or control its distribution.
- Never post any information that might make you or your property vulnerable, e.g., your address or travel plans.
- Wait until you get home to post your vacation blog and photos. If you do publish photos on the Internet first remove the geotags with a metadata removal tool.
- Not to click on any links, videos, programs, etc. provided in messages, even if a "friend" encourages you to click on them.
- Get program updates from the company's website, not through a provided link.
- Customize your personal privacy settings so only your friends have access to the information you post. Default settings on many sites allow anyone to see information about you. And check your settings frequently because they could be compromised when the site is updated, e.g., when new features are added.
- Read your network's privacy policy regularly to stay informed on how it uses or discloses your information. Choose to opt out of information sharing wherever possible.
- Scan your computer regularly with updated anti-virus, anti-spyware, and anti-adware programs.
- Know who your friends are and be careful about accepting and adding new ones. Be very cautious about revealing information about yourself if you chat with people you don't know.
- Be suspicious of anyone, even a "friend," who asks for money over the Internet.

**Illegitimate Websites**

Cybercriminals are now creating illegitimate websites that will receive high search-engine rankings and thus attract the attention of persons searching for information on a particular subject. Persons just visiting those sites risk having their computers infected with malware. And if they click on any links in those sites they risk becoming a victim of identity theft and various scams, e.g., ones that claim you can make a lot of money for a small initial investment. To avoid these problems users should:

- Keep your computer's anti-virus, anti-spyware, and anti-adware systems up to date with the latest firewalls and software.
- Use caution clicking on links that claim to provide videos or information on hot topics in the current news, e.g., the earthquakes in Haiti and Chile. And be aware that the bad guys are now tricking Google into telling you that the link is a PDF file, which makes it look more authentic.
- Do not click on links to other websites. Look up the address elsewhere and retype it into your browser.

- Check to see where you would actually go before you click on a link. You can do this by scrolling your mouse over the link and reading the address in the box that will pop up over the link. Do not click on the link if this address does not match the one in the link.
- Use the tips provided above to counter phishing.

Do the following to make sure a website is legitimate, especially if you are planning to make a purchase of a name brand product:

- Check that the domain name is spelled correctly. Cyber criminals are known to engage in type- or cyber-squatting to lure unsuspected victims to fake websites where they try to obtain personal and financial information or install malware on the victim's computer. They would use a name Appple.com or Bestbuyh.com. The fake website would be designed to look like the real one. It might offer a discount coupon in exchange for personal information or a credit card number.
- Check that the domain name ends in **.com**, **.org**, or **.net**. Those ending in **.cn** for China or **.mn** for Mongolia are likely to be fraudulent.
- Call the phone number posted and talk to a live person.

**E-card Dangers**

You receive an e-mail saying "A friend has sent you an e-card." The e-mail appears to be from a legitimate card company, but malware is downloaded into your computer when you click the link to see the card. You should delete the e-mail if you don't recognize the sender or if you are instructed to download an executable program to view the e–card. And make sure your computer has adequate anti-virus, anti-spyware, and anti-adware protection.

And even if you recognize the sender your computer could be harmed if the incoming e-mail is phony and you click on a link to an e-card or open an attachment. This happened around Christmas time in 2010 when employees of various government agencies received phony holiday messages that appeared to come from the White House.

**Unsafe Drugs from Online Pharmacies**

Buying prescription drugs on the Internet is easy but finding a safe source is not. There are thousands of Internet drug outlets selling low-price prescription medications that may be counterfeit, contaminated, or otherwise unsafe. Many of these outlets are located outside the United States, do not require a valid prescription, offer foreign drugs or ones not approved by the U.S. Food and Drug Administration, have unsecure websites, do not provide a way to contact a licensed pharmacist by phone to answer questions, and do not comply with state and federal laws and/or the patient safety and pharmacy practice standards of the National Association of Boards of Pharmacy (NABP).

You can avoid the risks of dealing with these rogue websites, which constitute about 96 percent of those on the Internet, by using safe sources have been identified by the NABP in its Verified Internet Pharmacy Practice Sites (VIPPS) program. They are listed as Recommended Internet Pharmacies on its website at **www.nabp.net**. These sites have undergone and successfully completed the NABP's accreditation process that includes a review of all policies and procedures regarding the practice of pharmacy and dispensing of medicine over the Internet as well as an on-site inspection of facilities used by the site of receive, review, and dispense medicine. The NABP website also lists Not Recommended Internet pharmacies and sites that have received its e-Advertiser Approval. These sites offer only limited pharmacy services or other prescription drug-related services. They have also been found to be safe, reliable, and lawful.

**Safe Cyber Practices**

There are presently two similar efforts by the U.S. Government to promote safer use of the Internet. The one by the FTC's Bureau of Consumer Protection is called *Stop.Think.Click*. The other, developed by a group representing industry, government, academia, and the nonprofit sector in 2009, and promoted by the Obama administration and the Department of Homeland Security, is called *Stop.Think.Connect*.

*Stop.Think.Click* defines seven practices for safer computing and provides tips on preventing identity theft, safe use of social networking sites, online shopping, Internet auctions, avoiding scams, and wireless security. It also provides a glossary of terms. The seven practices are:

1. Protecting your personal information
2. Knowing who you're dealing with
3. Using anti-virus and anti-spyware software, as well as a firewall
4. Setting up your operating system and web browser software properly, and updating them regularly
5. Protecting your passwords
6. Backing up your important files
7. Learning who to contact if something goes wrong online.

Go to **www.ftc.gov/bcp/edu/pubs/consumer/tech/tec15.pdf** for information about these practices and tips.

*Stop.Think.Connect* suggests that users do the following:

- Stop. Before you use the Internet take time to understand the risks and learn how to spot potential problems
- Think. Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact the safety of yourself and your family.
- Connect. Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

You can learn how to become a partner in this effort by going to its website at **www.stopthinkconnect.org**. This site also contains the tips and advice for doing the following.

Keeping a clean machine:

- Have the latest security software, web browser, and operating system.
- Use programs that automatically connect and update your security software.
- Protect all devices that connect to the Internet from all kinds of malware.
- Use your security software to scan all USBs and other external devices before attaching them to your computer.

Protecting your personal information:

- Secure your accounts with protection beyond passwords that can verify your identity before you conduct business.
- Use passwords that are more than eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol.
- Use different passwords for every account.
- Keep a list of your passwords stored in a safe place away from your computer.
- Use privacy and security settings to limit who you share information with.

Connecting with care:

- Delete any suspicious e-mail, tweets, posts, and online advertising.
- Limit the business you conduct from Wi-Fi hotspots and adjust your security settings to limit who can access your computer.
- Use only secure websites when banking and shopping, i.e., ones with **https://** or **shttp://** in their addresses.

Being web wise:

- Keep pace with new ways to stay safe online by checking trusted website for the latest information.
- Think before you act when you are implored to act immediately, offered something that sounds too good to be true, or asked for personal information.
- Back up your valuable information by making an electronic copy and storing it in a safe place.

Being a good online citizen:

- Practice good online safety habits.
- Post about others as you would have them post about you.
- Report all types of cybercrime to you local law enforcement agency and other appropriate authorities.

**WI-FI HACKING AND HOTSPOT DANGERS**

Use of Wi-Fi in coffee shops, libraries, airports, hotels, universities, and other public places pose major security risks. While convenient, they're often not secure. You're sharing the network with strangers, and some of them may be interested in your personal information. If the hotspot doesn't require a password, it's not secure. If it asks for a password through your browser simply to grant access, or it asks for a Wired Equivalent Privacy (WEP) password, it's best to treat it as unsecured. You can be more confident that a hotspot is secure only if it asks for the Wi-Fi Protected Access (WPA and WPA2) password. WPA2 is more secure. However, a flaw in a feature added to Wi-Fi called Wi-Fi Protected Setup (WPS) allows WPA and WPA2 security to be bypassed and broken by brute force in many situations.

Also, unsecure laptops and smart phones make it easy for a hacker to intercept information to and from the web, including passwords and credit- or debit-card numbers. They are also vulnerable to virus and spyware infections, and to having their contents stolen or destroyed. A hacked laptop or smart phone can also create a security risk for the user's workplace if it contains a password to the corporate network. Wi-Fi users should take the following steps to reduce these risks:

- Turn the Wi-Fi on your laptop, PDA, and smart phone off when you aren't using the network. Otherwise your Wi-Fi card will broadcast your Service Set Identifier (SSID) looking for all networks it was previously connected to. This enables hackers to figure out the key that unscrambles the network password.
- Use a known service instead of Free Public Wi-Fi or similar risky, unknown signals called ad hoc networks.
- Check the Wi-Fi security policies of your service provider and install the protections they offer to ensure it's a known network and not an "evil twin" hacker site pretending to be the legitimate one.
- Pay attention to warnings that a Secure Sockets Layer (SSL) certificate is not valid. Never accept an invalid certificate on a public wireless network. Log off and look for a trustworthy network. Look for the padlock indicating an SSL connection. Keep your firewall on. And keep your operating system updated.
- Find out if your company offers a Virtual Private Network (VPN) and learn how to use it. Encrypted VPN sessions offer the highest security for public wireless use. Use Hypertext Transfer Protocol Secure (HTTPS) when accessing a website or use a VPN to protect the transmission of sensitive information when using a wireless connection.
- Upgrade your Wi-Fi cards. The older WEP security is easily hacked. The new WPA and WPA2 are much more resistant to attack.
- Secure IEEE 802.11 wireless access points with a WPA2 and Advanced Encryption Standard (AES) encryption to protect sensitive communications.
- If your router has the WPS function, disable it. Methods have been published for doing this for some models. But on others, disabling the WPS in the user interface is not effective and the device remains vulnerable to attack.
- Learn to connect securely. Even the vulnerable WEP offers more privacy and protection than an unsecured public connection. It's not something the average hacker can crack. Look at your connection page for a name and description. A legitimate wireless network is simply called a "wireless network." It will display an icon of just one connected computer. So called ad hoc or peer-to-peer networks that are used by scammers to steal your personal information scammers are not legitimate. The will be called "computer-to-computer" networks and display an icon of several computers connected together. Never connect to this network. And be sure to set up your computer so it doesn't automatically connect to a network but allows you to choose a connection.
- Only log in or send personal information on website pages that are encrypted. They will have **https://** or **shttp://** in their URLs and a "lock icon" at the top or bottom of your browser window. You can click on this icon to display information about the website and help you verify that it's not fraudulent.
- Use a different password for each account.
- When you've finished using an account, log out. Don't stay signed in.

- Pay attention to warnings from your browser if you try to visit a fraudulent website or download a malicious program.
- Remove all passwords and browsing history after using a shared computer.
- Disable file-sharing on your laptop.
- Don't send any sensitive personal or business information while in a hotspot unless you absolutely have to.
- Put strong passwords on your wireless network. Passwords should be more than eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol. Other advice on creating strong passwords can be found at **www.microsoft.com/protect/yourself/password/checker.mspx**.
- In shopping, it's fine to browse website when you're out but wait until you are at home to do any online business.
- Be aware of the existence of malware that enables a mobile phone to be used as an open microphone with or without the owner's knowledge.

**CYBER SECURITY FOR BUSINESSES**

Computer crimes involve the illegal use of or the unauthorized entry into a computer system to tamper, interfere, damage, or manipulate the system or information stored in it. Computers can be the subject of the crime, the tool of the crime, or the target of the crime.

As the subject of a crime, a criminal would use your computer or another computer to willfully alter the information stored in your computer, add fraudulent or inaccurate information, delete information, etc. Motives for this include revenge, protest, competitive advantage, and ransom.

As the tool of a crime, a criminal would use a computer to gain access to or alter information stored on another computer. In one common mode of attack a hacker would send a "spear phishing" e-mail to employees who have access to the business bank account. The e-mail would contain an infected file or a link to a malicious website. If an employee opens the attachment or goes to the website, malware that gives the hacker access bank account log-ins and passwords would be installed on the computer. The hacker would then have electronic payments made to accounts from which the money would be withdrawn. Criminals also use computers to commit various frauds and steal identities and other information.

As the target of a crime, computers and information stored in them can be stolen, sabotaged, or destroyed. Sabotage includes viruses, malware, and denial-of-service attacks. Trade secrets and sensitive business information stored in computers can be lost in these kinds of attacks.

Your computers and the information in them should be protected as any valuable business asset. The following tips deal with physical and operational protective measures, Wi-Fi hacking and hotspot dangers, personnel policies and employee training, anti-virus and spyware protection, protecting your bank accounts, use of social media, preventing and dealing with data breaches, and safer use of the Internet. For more details see National Institute of Standards and Technology (NIST) Interagency Report NISTIR 7621 entitled *Small Business Information Security: The Fundamentals*, dated October 2009. It's available online under NIST IR Publications on **http://csrc.nist.gov**.

Also, consider joining the FBI's InfraGard, a partnership with the private sector with the goal of promoting an ongoing dialogue and timely communications between its members and the FBI. Its members gain access to information that enables them to protect their assets from cyber crimes and other threats by sharing information and intelligence. Go to **www.infragard.net** to apply for membership.

**Physical Protective Measures**

- Do not allow unauthorized persons to have access to any of your computers. This includes cleaning crews and computer repair persons.
- Install surface or cable locks to prevent computer equipment theft.
- Install computers on shelves that can be rolled into lockable furniture when employees leave their work areas.
- Locate the computer room and data storage library away from outside windows and walls to prevent damage from external events.

- Install strong doors and locks to the computer room to prevent equipment theft and tampering.
- Reinforce interior walls to prevent break-ins. Extend interior walls to the true ceiling.
- Restrict access to computer facilities to authorized personnel. Require personnel to wear distinct, color-coded security badges in the computer center. Allow access through a single entrance. Other doors should be alarmed and used only as emergency exits.

**Procedural and Operational Protective Measures**

- Classify information into categories based on importance and confidentiality. Use labels such as "Confidential" and "Sensitive." Identify software, programs, and data files that need special access controls. Employee access should be limited to what he or she needs to do their jobs. No employee should have unlimited access.
- Install software-access control mechanisms. Require a unique, verifiable form of identification, such as a user code, or secret password for each user. Install special access controls, such as a call-back procedure, if you allow access through a dial-telephone line connection.
- Have your Information Technology (IT) manager change administrative password on a regular basis. A number of free tools are available for this if manual modification is not practical. This password should also be changed during non-business hours.
- Require that passwords be a random sequence of more than eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol. Passwords should be changed at least every three months and not be shared.
- Employee user accounts should not have administrative privileges. This will prevent the installation of any unauthorized software or malicious code that an employee might activate.
- Change security passwords to block access by employees who change jobs, leave, or are fired. The latter become a high risk to your business for revenge or theft.
- Encrypt confidential data stored in computers or transmitted over communication networks. Use National Institute of Standards and Technology (NIST) data encryption standards.
- Design audit trails into your computer applications. Log all access to computer resources with unique user identification. Separate the duties of systems programmers, application programmers, and computer programmers.
- Review automated audit information and control reports to determine if there have been repeated, unsuccessful attempts to log-on both from within and outside your facility. Look for unauthorized changes to programs and data files periodically.
- Use monitoring or forensic tools to track the behavior of employees suspected of malicious activities.
- Monitor incoming Internet traffic for signs of security breaches.
- Make backup copies of important business information, i.e., documents, spreadsheets, databases, files, etc. from each computer used in your business. This is necessary because computers die, hard disks fail, employees make mistakes, malicious programs can destroy data, etc. Make backups automatically at least once a week if possible. Test the backups periodically to ensure that they can be read reliably. Make a full backup once a month and store it in a protected place away from your business.
- Delete all information stored in your printers, copiers, and fax machines at least once a week. Use a secure data deletion program that will electronically wipe your hard drives. Simply hitting the delete key will leave some data on the hard drive.
- Be careful in getting outside help with computer security problems. Call the San Diego District Office of the U.S. Small Business Administration at **(619) 727-4883** for advice and recommendations. Start with a list of vendors or consultants. Then define the problem, send out a request for quotes, examine each quote, and check the provider's references and history before hiring one.
- If you become a victim of Internet fraud or receive any suspicious e-mails you should file a complaint with the Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center (NW3C), at **www.ic3.gov**. The IC3 website also includes tips to assist you avoiding a variety of Internet frauds.

**Wi-Fi Hacking and Hotspot Dangers**

Your IT manager should also do the following to protect corporate data from hotspot dangers:

- Establish and enforce strong authentication policies for devices trying to access corporate networks.
- Require employees to use a corporate VPN and encryption when making connections and exchanging data. Better still, set up computers so that devices automatically connect to the VPN and encrypt data after making sure that the computer or device hasn't been lost or stolen.
- Make sure all devices and software applications are configured properly and have the latest patches.
- Ensure that corporate security policies prevent employees from transferring sensitive data to mobile devices or unauthorized computers.
- Provide employees with broadcast air cards that require a service plan so they don't have to use public hotspots for wireless connections.

**Personnel Policies and Employee Training**

Employees can do a great deal of damage to a business by ignorance of security policies, negligence in protecting business secrets, deliberate acts of sabotage, and the public release of sensitive information. The following measures will help prevent this.

- Conduct a comprehensive background check on prospective employees. Check references, credit reports, criminal records, and schools attended.
- Interview prospective employees. Seek to hire individual who are team-oriented, can respond well to criticism, and can deal well with conflicts, i.e., ones unlikely to become insider threats.
- Require vendors, suppliers, and other contractors to use similar standards in hiring their employees. Include language in all contracts that makes contractors liable for actions of their employees.
- Treat all employees fairly and make sure none are teased by their peers or supervisors because of their ethnicity, speech, financial situation, social skills, or other traits.
- Monitor activities of employees who handle sensitive or confidential data. Watch for employees who work abnormally long hours, weekends, or holidays, or who refuse to take time off. Many computer crime schemes require regular, periodic manipulation to avoid detection. Also watch for employees who collect material not necessary to their jobs, such as data printouts, software manuals, etc.
- Train your employees in your basic computer usage and security policies. Also cover penalties for not following your policies, and have employees sign a statement that they understand and will follow your policies.
- Train your employees about security concerns and procedures for handling e-mails, clicking on links to websites, responding to popup windows, and installing USB drives. For example, they should not open e-mail from an unknown sender, open unexpected e-mail attachments, click on any links in e-mail messages even if they look real, respond to popup windows, or install personal USB drives. As for USB drives, you should supply your employees with ones that have built-in encryption.
- Train your employees to be aware of what others are doing and to report any suspicious behavior that threatens your security.
- Conduct periodic re-training because people forget things. Use pamphlets, posters, newsletters, videos, etc.
- Prohibit your employees from using their work computers for online shopping. There is a chance that they might unwittingly land on a fake website with an address similar to that of a legitimate company, e.g., Appple.com instead of Apple.com. This would inadvertently expose your computer network to cyber attacks.

**Special Measures for Laptops**

Special security measures are needed for laptops to prevent them from being stolen and the data in them used to harm your business.

- Train employees in the need for special measures to protect laptops and their data wherever they may be used.
- Issue desktops instead of laptops to employees who seldom leave their offices.
- Have employees lock up their laptops when they are left unattended in their offices. Laptops should never be left unguarded.

- Have employees carry their laptops in a sports bag or briefcase instead of the manufacturer's bag.
- Do not leave a laptop visible inside vehicles or unattended in public places.
- If left unattended, secure the laptop with a cable lock to something that cannot be easily moved. Or install an alarm that will sound if the laptop is moved.
- Create a loss response team to monitor compliance with laptop and data security measures, investigate losses, assess data needs, and remove data no longer needed.

The following measures should be employed to protect your business in the event a laptop is lost or stolen.

- Have employees back up their files so they can be recovered if their laptop is lost or stolen. These back-up files should be kept in a separate, secure place.
- Protect data with strong passwords, i.e., ones that are at least eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol.
- Don't store passwords on laptops.
- Determine if employees need all the data on their laptops to perform their jobs. Remove any data that is not needed.
- Encrypt all sensitive information so it cannot be compromised.
- Install software that will enable you to erase sensitive information when the thief logs onto the Internet.

And the following measures can help you recover a laptop that has been lost or stolen.

- Keep a record of all laptop model and serial numbers so if one is recovered you can prove it is yours. Also keep the sales receipt and register the laptop with the manufacturer.
- Place stickers on the laptops with a phone number to call if one is lost and found by an honest person. But don't put the business name on it. That could be used by criminals to guess passwords or assess the sensitivity of the data stored on the laptop.
- Install hardware, software, or both to aid in recovery of the laptop. After you report the laptop lost or stolen the software enables a monitoring company to track the laptop when the thief logs onto the Internet. Hardware systems work the same but have a Global Positioning System (GPS) device that can pinpoint its location.
- Report the loss to the local law enforcement agency, and notify the manufacturer.
- Look for it on Craigslist and E-Bay.

**Protecting Bank Accounts**

- Set up dual controls so that each transaction requires the approval of two people.
- Establish a daily limit on how much money can be transferred out of your account.
- Require all transfers be prescheduled by phone or confirmed by a phone call or text message.
- Require that all new payees be verified.
- Check bank balances and scheduled payments at the end of every workday, rather than at the beginning, and contact the bank immediately if anything is amiss. Timely action can halt the completion of a fraudulent transaction because transfers usually aren't made until the next morning.
- Inquire about your bank's defenses against cyberattacks and review the terms of your banking agreement with regard to responsibilities for fraud losses. Shop around for banks that provide better protections.
- Conduct online business only with a secure browser connection, which is usually indicated by a small lock in the lower right corner of your web browser window. Erase your browser cache, temporary Internet files, cookies, and history after all online sessions. This will prevent this information from being stolen if your system is compromised.

**Use of Social Media**

While the use of social media can stimulate innovation, create brand recognition, generate revenue, and improve customer satisfaction, it has inherent risks that can negatively impact business security. Thus businesses need to develop a social media strategy and a plan to address these risks. Some risk mitigation techniques for business and employee use of social media are listed below. For details see the emerging technology white paper entitled *Social*

*Media: Business Benefits and Security, Governance and Assurance Perspectives* published by the Information Systems Audit and Control Association (ISACA).

- Ensure that anti-virus and anti-malware controls are updated daily.
- Use content filtering to restrict or limit access to social media sites.
- Establish policies for the use of mobile devices to access social media.
- Install appropriate controls on mobile devices.
- Conduct awareness training to inform employees of the risks in using social media.
- Provide employees with clear guidelines regarding what information about the business can be posted.
- Scan the Internet for unauthorized or fraudulent use of the business name or brand.

**Preventing and Dealing with Data Breaches**

The five key principles defined by the Federal Trade Commission in a paper entitled *Protecting Personal Information: A Guide for Business* at **http://business.ftc.gov/privacy-and-security/data-security** will help you protect personal information in your business and prevent data breaches. They are: (1) Take stock, (2) Scale down, (3) Lock it, (4) Pitch it, and (5) Plan ahead. You should do the following for each.

1. Take stock: Know what personal information you have in your files and in your computers.

- Inventory all file-storage and electronic equipment. Know where your business stores sensitive data.
- Talk to your employees and outside service providers to determine who sends you personal information and how it is sent.
- Consider all the personal information you collect from customers, and how you collect it.
- Review where you keep the information you collect, and who has access to it.

2. Scale down: Keep only what you need for your business.

- Use Social Security Numbers (SSNs) only for required and lawful purposes. Don't use them for employee or customer identification.
- Keep customer credit or debit card information only if you have a business need for it. Don't keep any information you don't need.
- Change the default settings on your software that reads customer's credit or debit cards.
- Review the credit application forms and fill-in-the-blank web screens you use to collect data from potential customers, and eliminate requests for any you don't need.
- Use no more that the last five digits of credit- or debit-card numbers on electronically printed receipts that you give to your customers. And don't use the card's expiration date.
- Develop a policy for retaining written records that is consistent with your business needs and the law.

3. Lock it: Protect the information that you keep and transmit.

- Keep documents and other materials containing personal information in locked rooms or file cabinets.
- Remind employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Create a security policy for your employees when using laptops in and out of your office. (See prior section on Special Measures for Laptops.)
- Control access to your building.
- Encrypt sensitive information you send over public networks or use a secure file transfer service. Don't send personal information by e-mail.
- Run up-to-date anti-virus and anti-spyware programs on all your computers. Use a firewall to protect your computers and network. (See prior section on Anti-virus and Spyware Protection.)
- Require employees to use strong passwords.
- Set access controls so employees only have access to information they need for their jobs. (See prior section on Procedural and Operational Protective Measures.)

4. Pitch it: Properly dispose of what you no longer need.

- Create and implement secure information disposal practices for employees in your office and for those who travel or work at home.
- Train your staff to separate sensitive and other paper records. Dispose of the former by shredding, burning, or pulverizing them. Use cross-cut shredders. The latter can be put in the trash.
- Make shredders available throughout your office, especially next to the copiers.
- Remove and destroy the hard disk of any computer or copier headed for the junkyard. Or wipe them securely.
- Remove and securely wipe hard drives of rented copiers before returning them. Or clear the memory and change the pass codes.
- Destroy CDs, floppies, USB drives, and other data storage devices, or securely wipe them before disposal.
- Test how thoroughly factory resets and remote wipes destroy data on any smartphones your employees use in the business, and only permit them to use phones on which the data can be completely destroyed when the device is retired. If there is any doubt about this, use a hammer on the phone to make sure it does not get into the secondary market.

5. Plan ahead: Create a plan for dealing with security breaches.

- Organize a response team and designate a team leader to manage the activities.
- Draft contingency plans for dealing with various kinds of breaches, including hacking, lost laptop, etc.
- Investigate breaches immediately and take steps to eliminate existing vulnerabilities or threats to personal information.
- Disconnect a compromised computer from the Internet.
- Post information about the breach on your website and include the phone number and e-mail address of your customer service staff.
- Create a list of who to notify inside and outside of your business in the event of a breach. The latter include the appropriate law enforcement agencies, the persons whose information has been compromised, your customers and other businesses that may be affected, and the media.
- Draft notification letters and other written communications. Consult your attorney for state and federal notification requirements.
- Consider what outside assistance is needed, e.g., in forensics, media relations, etc.

Note that California Civil Code Sec. 1798.82 requires businesses to notify persons whose personal information has been compromised and specify the information involved. The notice requirement is triggered if the breach involves a person's name in combination with any of the following: Social Security Number; driver's license or California Identification Card number; financial account, credit-card, or debit-card number along with any PIN or other access code required to access the account; medical information; or health insurance information. The letter of notice should also recommend measures to take to deal with the breach, warn of attempts to obtain personal information by e-mail, and ask that any such attempts be reported to your customer service staff immediately.

**CYBER SECURITY FOR CHILDREN**

Although the vast majority of online services and Internet material is legitimate and benign, there have been numerous incidents of children receiving pornographic material, providing personal information under the pretext of possibly winning a prize, or sending money for promised benefits or products. Warning signs of these dangers include excessive late-night computer use, secretive behavior about computer associates, hidden files or directories, and password-protected bios, files, or logical drives.

If you are not familiar with computers, the Internet, and social networking you should visit **www.NetSmartz411.org**, the premiere Internet-safety helpdesk and hotline, to help educate yourself. You should also sit down with your children to have them show you the websites they visit, how they navigate through the Internet, and how they use social networking sites. To better understand the latter you should try networking yourself. This is a great way to connect with your children on computer-related matters.

**Minimizing Internet Dangers**

Parents should do the following to minimize Internet dangers that your children may encounter:

- Start early. Talk to your children about online behavior, safety, and security as soon as they start using a computer, cell phone, or any mobile device. Supervise closely the choice of websites for young children. Continue to monitor online activities as your children get older and more independent.
- Set reasonable guidelines and time limits for Internet and cell phone use, and social networking. Prohibiting Internet use is not a good idea because it is too easy for children to establish accounts at a friend's house or many other places. But do set time limits on computer use. People, not computers, should be their best friends and companions.
- Keep the computer in the family room or other area where its use can be monitored. Don't allow computers and mobile devices such as laptops and smart phones to be used in your children's bedrooms. And don't allow your children to have separate passwords and log-on names.
- Post clear, simple, easy-to-read rules for Internet use on or near the computer. Discuss these rules with your children and make sure they understand the reasons for them. Visit **www.NetSmartz.org** for examples of rules and safety tips. Your supervision and attention is the best way to protect your children when using the Internet.
- Know what Internet access your children have away from home, i.e., at a friend's home, libraries, schools, and cell phones and other wireless devices, and have a plan to monitor their online activities there as well as at home.
- Initiate conversations with your children about their Internet use. Communicate your values, be patient and persistent, and don't rush through conversations. Encourage your children to come to you with any problems they encounter online.
- Make sure they understand the importance of password and privacy protection, and not to share passwords or log-on names with anyone else. And don't let them use their pet's names as passwords.
- Have your children request your permission to exchange phone numbers or meet another child they have "talked" to online. Consider talking to the other child's parents about a meeting and accompanying your child to the meeting, which should be in a public place. Tell your children that caution is needed because people online are not necessarily who they might seem to be.
- Discourage your children from visiting chat rooms, especially those with video, even if they claim to be child friendly. Persons who would harm children use these websites to entice children.
- Use filtering software to scan for offensive words and phrases in chat rooms and then end the conversations by signing off.
- Install a browser that limits the websites that your younger children can visit to those vetted by educational professionals. Some will send you periodic e-mails that detail you children's Internet activity.
- Install a monitoring service like McGruff SafeGuard. It's free and also scans any chat or text conversations for bad language and other inappropriate communications. Go to **www.gomcgruff.com** for details of this service.
- Have your children promise not to turn off any programs you might install to monitor their computer use.
- Understand how online services work.
- Check the computer's cache and history to see what websites have been accessed.
- Ask your children for their passwords and log-on names, and to share their blogs and online profiles with you. Be aware that they can have multiple accounts on multiple services. Search for you children's identifying information and monitor their screen name(s) and websites for inappropriate content. Also monitor their texts to make sure they are not receiving any threatening or harassing messages, or are sending, receiving, or saving any sexts.
- Learn the meaning of the acronyms your children use in texting. Go to **www.netlingo.com/acronyms.php** for a list of acronyms and their definitions, e.g., PAL means parents are listening.
- Make sure your child's screen name does not reveal any identifying information such as name, age, location, school. A screen name should be benign and innocuous, e.g., the first letter of each word in an easily-remembered phrase.
- Prohibit your children from downloading any games, movies, programs, etc., trying to win "free" things, or buying things without your permission.
- Tell your children it's not safe to put photos or any type of personally identifying information on a personal website without privacy settings, even if they promise to give the website address to people they know. Anyone in the world can access such a website. Also, personally identifying information should not be published on a

group website or in an Internet yearbook. Group photos are preferable to individual photos only if no names are published.
- Have your children ask permission before listing any adults as "friends" online, even if they are teachers, relatives, or your friends.

**Dangers of Social Networking**

Children who use social networking sites like Facebook and MySpace should be warned about online predators and harassers. They should be taught to do the following to prevent and deal with any problems that might arise:

- Never to give out your name, address, phone number, or any other personal information that can identify you. Avoid posting anything that would enable a stranger to find you, e.g., school names. Members' profiles become public information.
- Never say you are home alone.
- Don't post anything that you wouldn't want the world to know, especially anything or language that might embarrass you later, e.g., in applying for college or a job. What's uploaded can be downloaded and passed around by others and be posted online forever. It can't be taken back even if it's deleted from a site.
- Never send out any pictures of yourself, family members, or friends.
- Be careful about adding strangers to your list of "friends." People aren't always who they say they are.
- Come to me to discuss any harassment, hate speech, and inappropriate content you receive.
- Check comments regularly. Ignore and don't respond to any that are mean or embarrassing. Just log off if the harassment bothers you.
- Avoid misleading people into thinking you are older or younger than you are.
- Don't talk about sex or use any sexually explicit language.
- Block people from sending you messages or e-mail, or delete them from your "buddy list" if they harass you.
- Change your password if someone hacks into your profile. Change you username and e-mail address if someone repeatedly bothers you.
- Contact the company that runs the site to have any your profile deleted if it was created or altered without your knowledge.
- Talk to someone you trust if you are upset about what is being said about you. If you are scared or threatened contact a Juvenile Service Team officer at your nearest SDPD area station and inform your Internet Service Provider.

Children also need to be given rules for using cell phones and be warned of dangers in their use. Rules should deal with when and where phones can be used, what they can and cannot be used for, and etiquette and safety in texting. You need to set good examples in the use of phones, e.g., not while driving. One thing that phones should not be used for is sexting, i.e., the sending or forwarding of sexually explicit photos, videos, or messages. In addition to risking their reputation and friendships, they could be breaking the law if they create, forward, or even save this kind of message. The following are some good rules for texting.

- Be polite and respect others. Avoid using shorthand that might lead to misunderstandings. Think about how a message might be read and understood before sending it.
- Ignore messages from people you don't know.
- Block numbers of people you don't want to hear from.
- Don't post your cell phone number on the Internet.
- Never provide personal or financial information in response to a text message.
- Use Cc: and Reply all: with care.

**Cyberbullying**

Cyberbullying is another problem you should talk to your children about. You should tell them that they can't hide behind the messages they send or pictures they post, and that hurtful messages not only threaten the victim, but they make the sender look bad and can bring scorn from peers. Such messages are also a misdemeanor under California law for which the sender can be punished by up to one year in a county jail, by a fine of not more than $1,000, or

both. Also, you should also make sure your own conduct does not encourage bullying, i.e., that you don't make mean-spirited comments about others or act unkindly to them.

You also need to be prepared to help your children if they become a victim of bullying. You should encourage them to show you any online messages or pictures that make them feel threatened or hurt. If you fear for your child's safety you should call the SDPD on its non-emergency number, **(619) 531-2000** or **(858) 484-3154**. Otherwise tell your child not to respond, save the messages and pictures for evidence, and keep you informed. Call the SDPD again if the bullying persists. Here are some other things your child should do:

- Report the bullying to the website or network where it appears.
- Delete the bully from your list of "friends" or "buddies," or block the bully's username or e-mail address.
- Share these measures with a friend who is a victim of bullying. Bullying usually stops quickly when peers intervene on behalf of the victim.

**Reporting Attempted Sexual Exploitation**

Any suspected online sexual exploitation or attempt by an adult to meet your child should be reported immediately to the San Diego Internet Crimes against Children Task Force at **(858) 715-7100** and the Cyber Tipline at **www.cybertipline.com** or **(800) 843-5678**. The former is the local law-enforcement agency that deals with these matters. The latter is managed by the National Center for Missing and Exploited Children (NCMEC) and is mandated by Congress to forward your information to the appropriate law enforcement agency for investigation. If your children or anyone in your home receives pornography depicting children or your children receive sexually explicit images, report the imagery to ICAC and keep it open on your computer until an investigator comes to see it. Do not copy or download it. In the meantime you can use your computer for other things or turn your monitor off.

**Preventing Cyber Crimes**

Children should also be warned about virus creators, identity thieves, and spammers. These cyber-criminals are increasingly targeting users of social networking sites in an effort to steal their personal data and the passwords to their accounts. One of the tactics they use to gain access to this information involves sending social networking users e-mails that appear to come from online "friends." For example, some Facebook users have been receiving e-mails from "friends" that claim to contain a video of them. When they click on it they download a virus that goes through their hard drives and installs malware (malicious software). The virus, known as Koobface, then sends itself to all the "friends" on the victim's Facebook profile. A new version of the virus also is affecting users of MySpace and other social networking sites. Cyber-criminals are tricking social networking users into downloading malware by creating fake profiles of friends, celebrities, and others. Security experts say that such attacks, which became widespread in 2008, are increasingly successful because more and more people are becoming comfortable with putting all kinds of personal information about themselves on social networking sites. They warn that users need to be very careful about what information they post because it can be used to steal their identities.

To avoid these problems on social networking sites or anywhere in the Internet, you should warn your children to:

- Not to open any e-mail from an unknown sender. Delete it without opening it. "Drive-by spam" can automatically download malware when an HTML e-mail is opened. You don't have to click on a link or open an attachment to get infected.
- Not to click on any links, videos, programs, etc. provided in messages, even if a "friend" encourages you to click on them.
- Not to visit any sites that promise ways of bypassing parental controls or blocks set up by schools to prevent users from visiting sites such as Facebook. These sites are full of scams, malware, and offers for other services.
- Get program updates directly from the company's website, not through a provided link.
- Customize your personal privacy settings so only your "friends" have access to the information you post.
- Read your network's privacy policy regularly to stay informed on how it uses or discloses your information.
- Scan your computer regularly with an anti-virus program. Make sure the program is kept up to date, preferably automatically.
- Be suspicious of anyone, even a "friend," who asks for money over the Internet.

- Don't open or forward chain letters. Just delete them. They are nuisances at best and scams at worst. And many contain viruses or spyware.
- Watch out for "free" stuff. Don't download anything unless it's from a trusted source and it's been scanned with security software. "Free" stuff can hide malware.
- Do not buy or download free anti-spyware software in response to unexpected pop-ups or e-mails, especially ones that claim to have scanned your computer and detected malicious software.
- Make sure the pop-up blocker in the tools menu of your browser is turned on. This will prevent most pop-up ads. If you do get one, be careful in getting rid of it. Never click on any of its boxes. By clicking on No or Close you may actually be downloading malware onto your computer. And even clicking on the X in the upper right-hand corner can initiate a download instead of closing the ad. To be safe on a PC, hold down the Ctrl and Alt keys and hit Delete. Then in the Windows Security box click on Task Manger, and then click on End Task. This will clear your screen. Then run a full anti-virus scan.
- Avoid all online games and quizzes that request personal information, including your e-mail address. Providing this information can put your identity at risk.

**Additional Information**

Additional information on Internet dangers to children and how to keep children safe online is available on numerous websites. These include the following:

- San Diego Internet Crimes Against Children Task Force at **www.sdicac.org**
- National Cyber Security Alliance at **www.staysafeonline.org**
- San Diego County District Attorney at **www.sdcda.org. S**ee the Protecting Children Online page under Protecting the Community.
- GetNetWise at **www.GetNetWise.org**
- Federal Bureau of Investigation at **www.fbi.gov**. See *A Parent's Guide to Internet Safety* under Cyber Issues on the Reports and Publications page.
- NCMEC at **www.ncmec.org**. See resources for parents and guardians.
- NET CETERA: Chatting with Kids about Being Online at **www.onguardonline.gov**.
- *Living Life Online* at **http://www.ftc.gov/bcp/edu/microsites/livinglifeonline/index.shtm**.

**Protecting Your Children's Identities**

- Provide your child's Social Security numbers only when it is required by a government agency or financial institution. Never provide it for identification.
- Carry your child's Social Security number or card in your purse or wallet only when you know you will need it.
- Teach your children never to give out personal information over the phone or on the Internet.
- Check to see if any of your children have a credit report by visiting **www.AnnualCreditReport.com** or calling **(877) 322-8228**, a service created by Equifax, Experian, and TransUnion, the three nationwide consumer-reporting companies. No report should exist unless someone has applied for credit using your child's Social Security number. No minor should have a credit report. At a FTC-sponsored forum on child-centric fraud in July 2011 it was estimated that more than 140,000 American children become victims of identity theft each year. By various means thieves obtain children's SSNs and sell these genuine numbers to persons with poor credit ratings who obtain credit cards, make extensive purchases, and don't pay their bills. If this happens you should contact the credit card companies and the three nationwide consumer credit reporting bureaus immediately.
- Watch your children's mail for credit card applications, bills, or bank statements. They are signs that someone has started a credit history in your child's name.
- Request that banks in which your children have accounts remove their names from marketing lists.
- Report any suspected identity theft to the three nationwide consumer reporting companies and obtain copies of any credit reports in your child's name and Social Security number. If your child does have a credit report ask to have all accounts, application inquiries, and collection notices removed immediately. Tell the credit issuer that the account is in the name of your minor child who by law isn't permitted to enter into contracts.
- Take advantage of your rights under the federal Children's Online Privacy Protection Act (COPPA). This law requires websites to get parental consent before collecting and sharing information from children under 13.

COPPA covers sites designed for children under 13 and general audience sites that know certain users are under 13. It protects information that websites collect upfront and information that children give out or post later. It also requires these sites to post a privacy policy that provides details about the kind of information they will collect and what they might do with the information. You should: (1) know your rights, (2) be careful with your permission, (3) check out the sites your children visit, (4) review the sites' privacy policies, (5) contact the site if you have any questions about its privacy policy, and report any site that breaks the rules to the FTC at **www.ftc.gov/complaint**. For answers to frequently asked questions about the Children's Online Privacy Protection Rule go to **http://www.ftc.gov/privacy/coppafaqs.shtm**.